Security Hardening in Building Networks

Challenges in making Building Networks secure from inside and outside threads and how we can manage this

Presenter

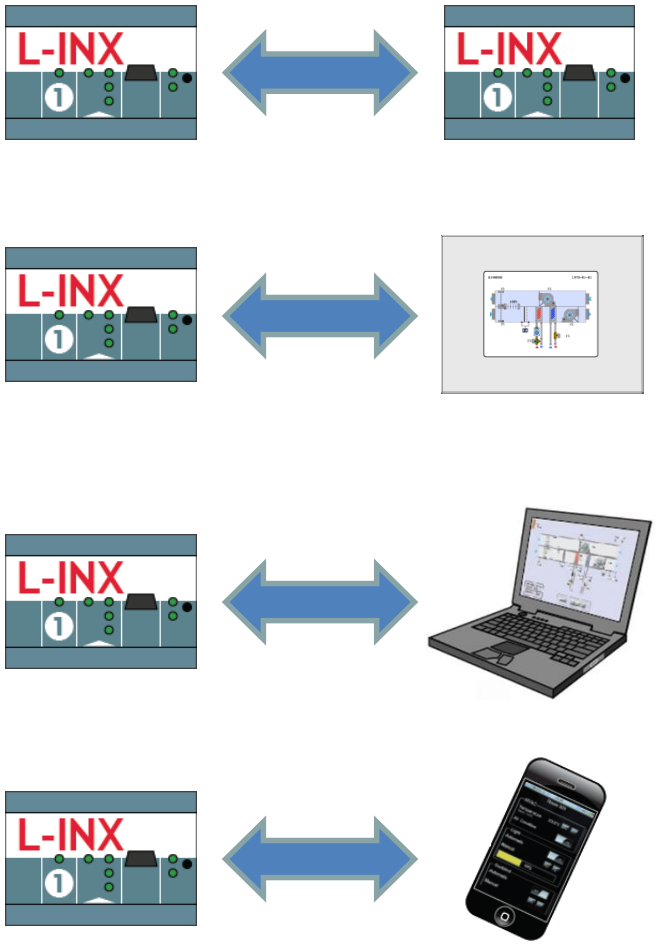
- Hans-Jörg Schweinzer
  - LOYTEC Founding Partner and CEO
  - Marketing, Business Development, Sales
- Involvement
  - Fieldbus and Internet technology for more than 25 years
  - Active in CEN TC247, ISO TC205, CENELEC TC205

Overview

- Motivation
- Security Threats
- Network Security
- Secure Protocols
- System Hardening
- Secure Mode

Motivation

- Internal comm
  - IP-based protocols
  - IT components
  - Controller to controller
  - Controller to panels
- External comm
  - Mobile devices
  - Web Access
  - BMS Access



Threats in The Press

- Stuxnet on Iranian Centrifuge
  - Worm infecting industrial controller equipment
  - IEEE Spectrum – The Real Story of Stuxnet
- Marvel of connectivity illustrates new cyber risks
  - Hackers focus on Internet-connected control systems
  - July 12, 2012
- Botnet captures routers
  - Malware on Routers for spying on traffic (report passwords)
  - c't 21, 2013

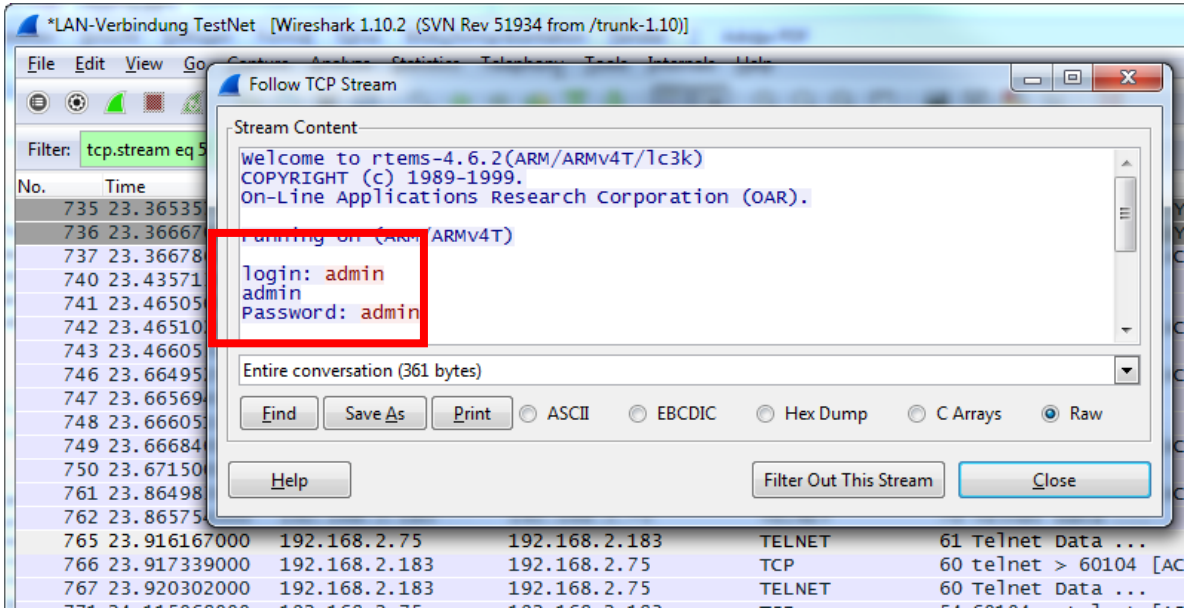
IEEE SPECTRUM

The Washington Post

heise Security

Threats: Clear-Text

- Clear-Text
  - Read user/password (break-in)
  - Record usage behavior (burglars)



Threats: Replay

- Replay

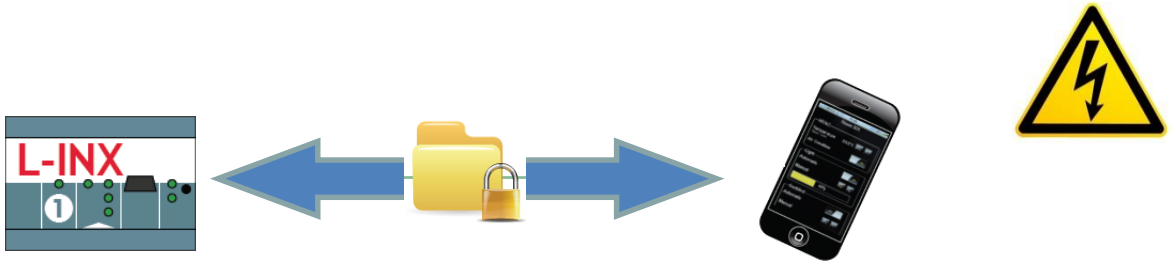
63	2.585755000	192.168.24.250	192.168.2.75	TCP	60 http > 55513 [ACK] Seq=1 A
64	2.585785000	192.168.2.75	192.168.24.250	HTTP/XML	654 POST /DA HTTP/1.1
65	2.586292000	192.168.24.250	192.168.2.75	TCP	60 http > 55513 [ACK] Seq=1 A

```
Frame 64: 654 bytes on wire (5232 bits), 654 bytes captured (5232 bits) on interface 0
Ethernet II, Src: DigitalD_95:56:c4 (00:11:6b:95:56:c4), Dst: LoytecEl_02:7c:39 (00:0a:b0:02:7c:39)
Internet Protocol Version 4, Src: 192.168.2.75 (192.168.2.75), Dst: 192.168.24.250 (192.168.24.250)
Transmission Control Protocol, Src Port: 55513 (55513), Dst Port: http (80), Seq: 327, Ack: 1, Len: 600
[2 Reassembled TCP Segments (926 bytes): #62(326), #64(600)]
Hypertext Transfer Protocol
eXtensible Markup Language
  <?xml
  <soap:Envelope
      xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <soap:Body>
      <Write
          xmlns="http://opcfoundation.org/webservices/XMLDA/1.0/"
          ReturnValuesOnReply="true">
        <Options
        <ItemList
            ItemPath="">
          <Items
              ItemPath=""
              ItemName="User Registers.LightsOn"
              ClientItemHandle="34444320">
            <Value
                xsi:type="xsd:boolean">
              false
            </Value>
```

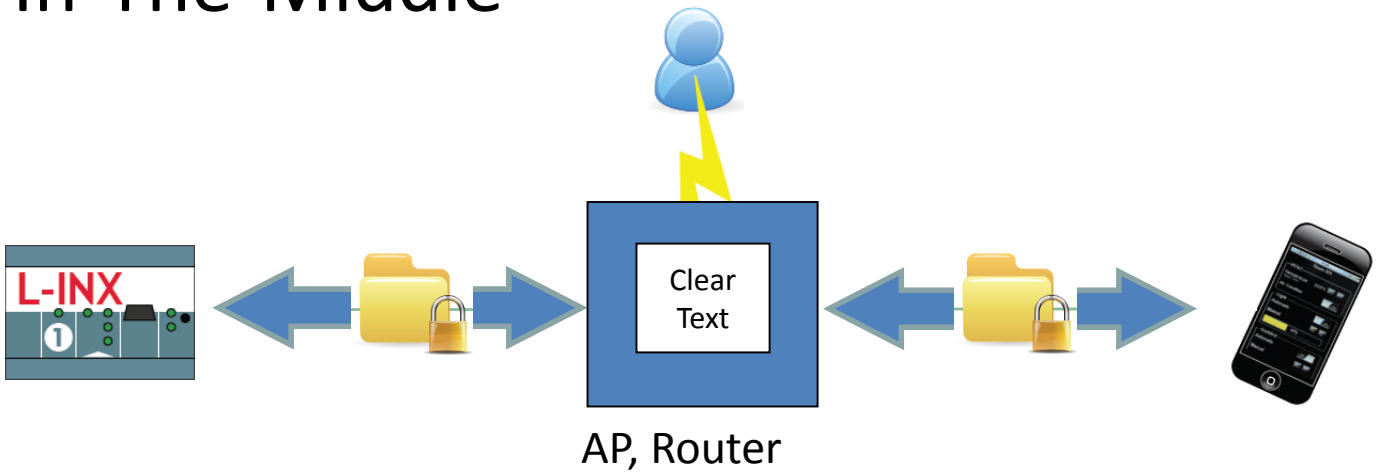
- Web Service
- CEA-852
- BACnet/IP

Threats: Man-In-The-Middle

- Secure Traffic



- Man-In-The-Middle

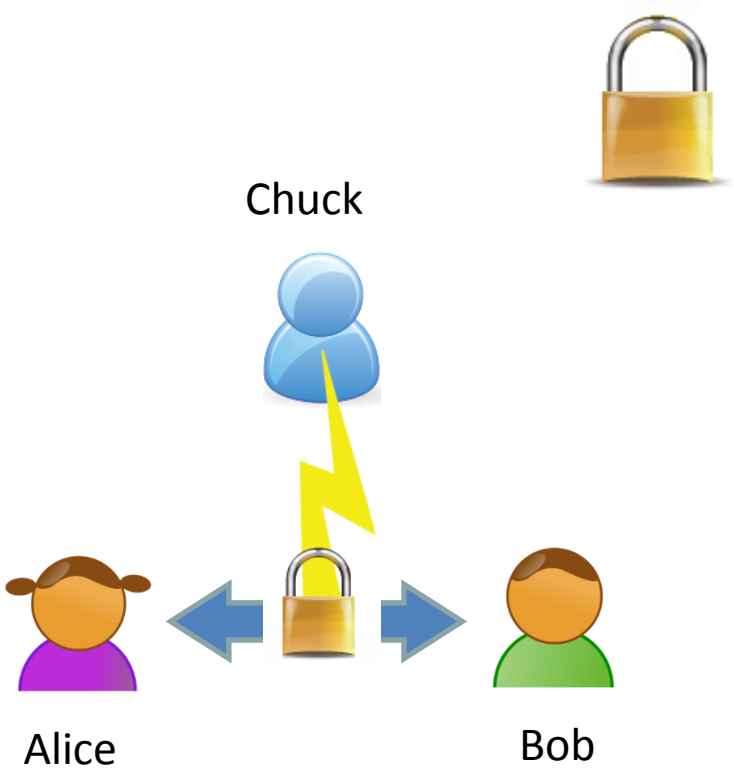


Threats: Exploits

- Denial of service
  - Keep device from productive function
  - Use open ports
  - Exploit vulnerability (e.g. reboot)

Security

- Communication
  - Integrity
  - Confidentiality
  - Authenticity
  - Non-Repudiation
- System
  - Strong passwords
  - Restrict access



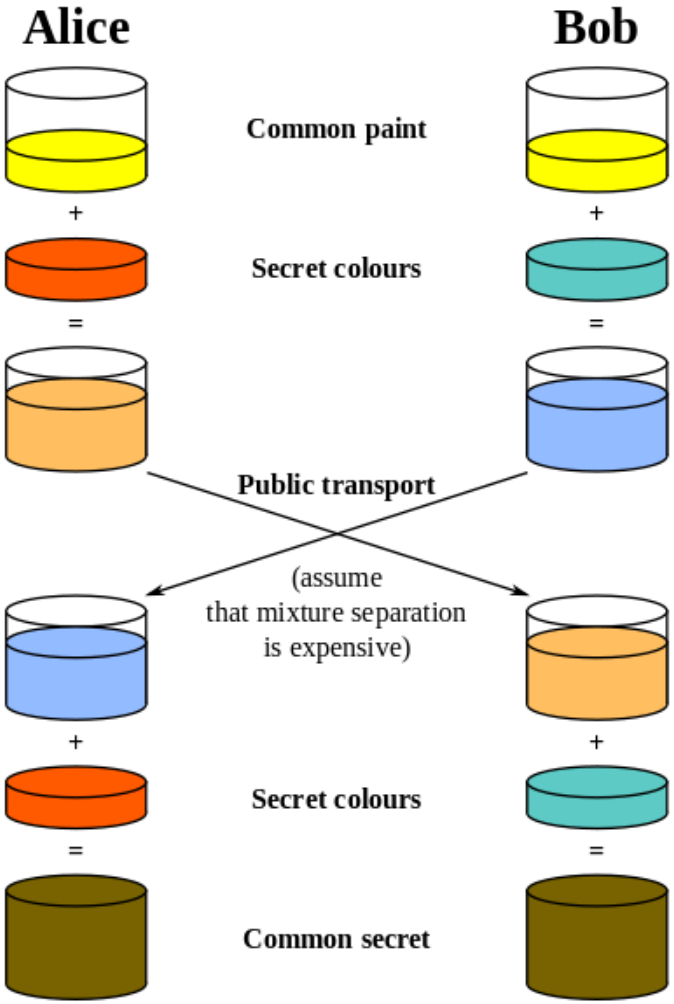
Integrity

- Message integrity
  - Verify message is not altered in transit from Alice to Bob
  - Message Authentication Code (MAC) with shared secret
  - Non-transmitted secret
  - Secure one-way digest function: MD5, SHA1
  - Fingerprint check

Confidentiality

- Encryption
  - No clear-text: Chuck cannot read
  - Passwords are confidential
  - Prevent eavesdropping on control data
- Stream Cipher
  - Encryption key (symmetric)
  - Must be secret!
  - Pre-shared
  - Key exchange between Alice and Bob

Establish a Secret



Diffie-Hellman
Key Exchange

Digital Signature

- Asymmetric Cryptography
  - Private key is secret (!)
  - Public key to anyone
  - Complete operation needs both keys
- Digital Signature
  - Detect forgery and tampering
  - Prove origin of message (authentication)
  - Sender cannot deny (non-repudiation)
  - Message fingerprint encrypted w/private key
  - Verify: Use public key and compare

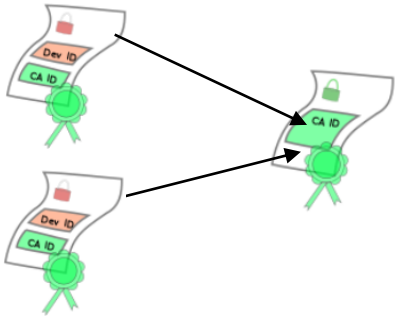
Certificate

- Public-key certificate
  - Document with digital signature
  - Bind public key to identity
- Information

Installed Server certificate (Self-signed)	
RSA Key Size	1024
Validity Start Date	2013-09-17
Validity End Date	2023-09-15
Common Name	loytec.local
Organization Name	LOYTEC electronics GmbH
Organization Unit	Development
City	Vienna
State	Vienna
Country	AT
MD5 Fingerprint	49:B6:4D:79:DD:EF:77:4F:F2:35:BF:6D:47:B3:D8:54
SHA1 Fingerprint	D6:AE:4D:DF:AD:3A:16:2A:57:58:40:3E:8A:55:4F:63:C2:B1:AA:1F

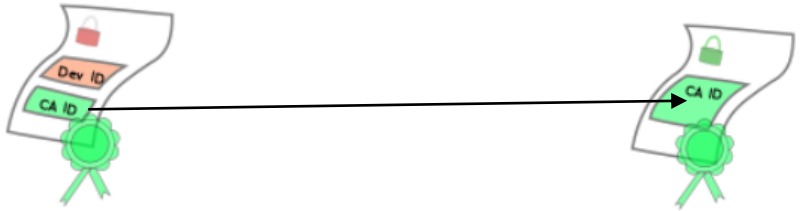
Public Key Infrastructure

- X.509 certificates
  - Standardized format
  - Common name identifies server
  - Validity period
- Self-signed certificate
  - Trust Server by Server
- Web of trust
  - Trust certificate authority
  - Sign server certificate by CA
  - Server + CA certificates



Trust Certificates

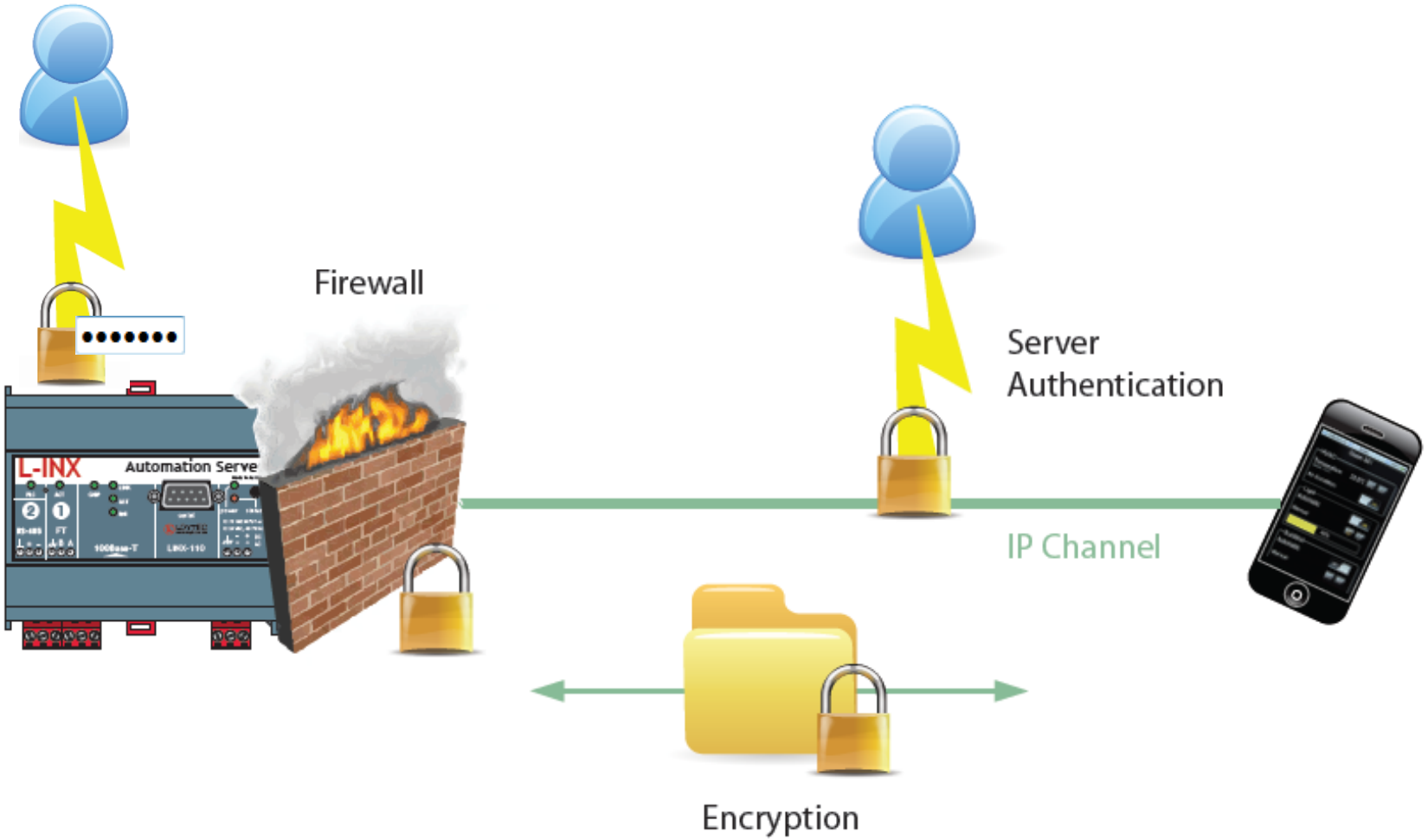
- Trust CA certificate



- Verify device by server certificate

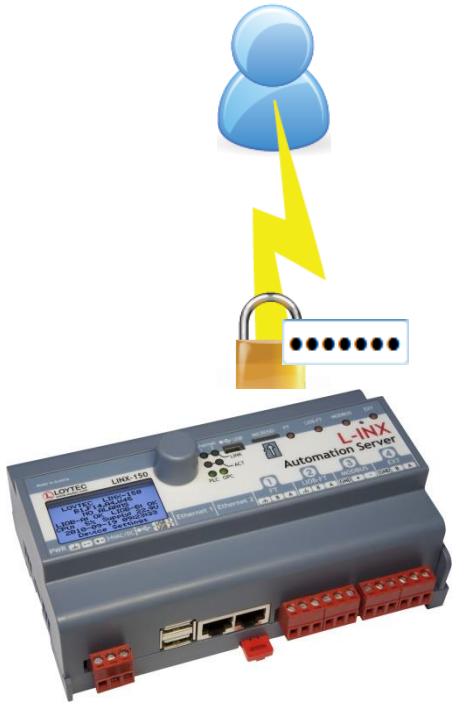
- Establish communication with server

System Hardening



User Restrictions

- Change The Password (!)
  - Admin/Operator/Guest Users
  - PIN Protection on LCD
  - Use Strong Password
    - not admin, 123, asd
  - Practice Memorize Sentence:
    - LINX security is good for you!
    - → Lsig4u!



www.defaultpassword.com

default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

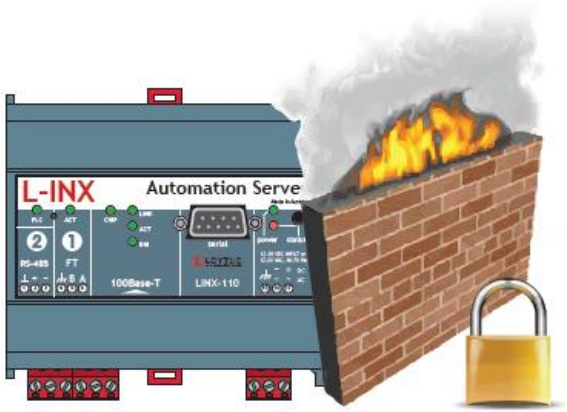
Displaying 78 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
Lanier	5618		Multi	(none)	sysadm
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	access
Lantronics	Lantronics Terminal Server		TCP 7000	n/a	system
Lantronix	Lantronix Terminal		TCP 7000	n/a	lantronix
lawl yo			HTTP	a	b
LdxWXAzNx	xXTGryMUTUScSdRuINI	JetiximZAWXFn		WbvCndpRn	vYetbYhpeyd
Leading Edge	PC BIOS		Console	n/a	MASTER
LeXKceHcgNSOo	ArOpIQXYqsGYTyMIJ	dFhnHHBxm		ljtNZgYHQ	MNhtdCzEregq
LG	mobile handset		Multi	vikram	singh
LgKwakiJHCuGnQg	QCEfjlpLn	wfpkvAiHJl		MALwKkjSQ	PenBZiOJiNngAtNnV
lgwLRDhWeOs	qXIfGICGTSHUdiFu	LGpYMlDRfKdxOadUR	SSH	9688	rK2VV7Ku
LHDDrASZcoahZjVRNBq	XuueWgSUg	DCBIcCtyFLmILNpPgl	SNMP	12728	vhsOPuXl
Linksys	BEFW11S4	1	HTTP	admin	(none)
Linksys	DSL		Telnet	n/a	admin
Linksys	E3000	1.0	HTTP	admin	admin

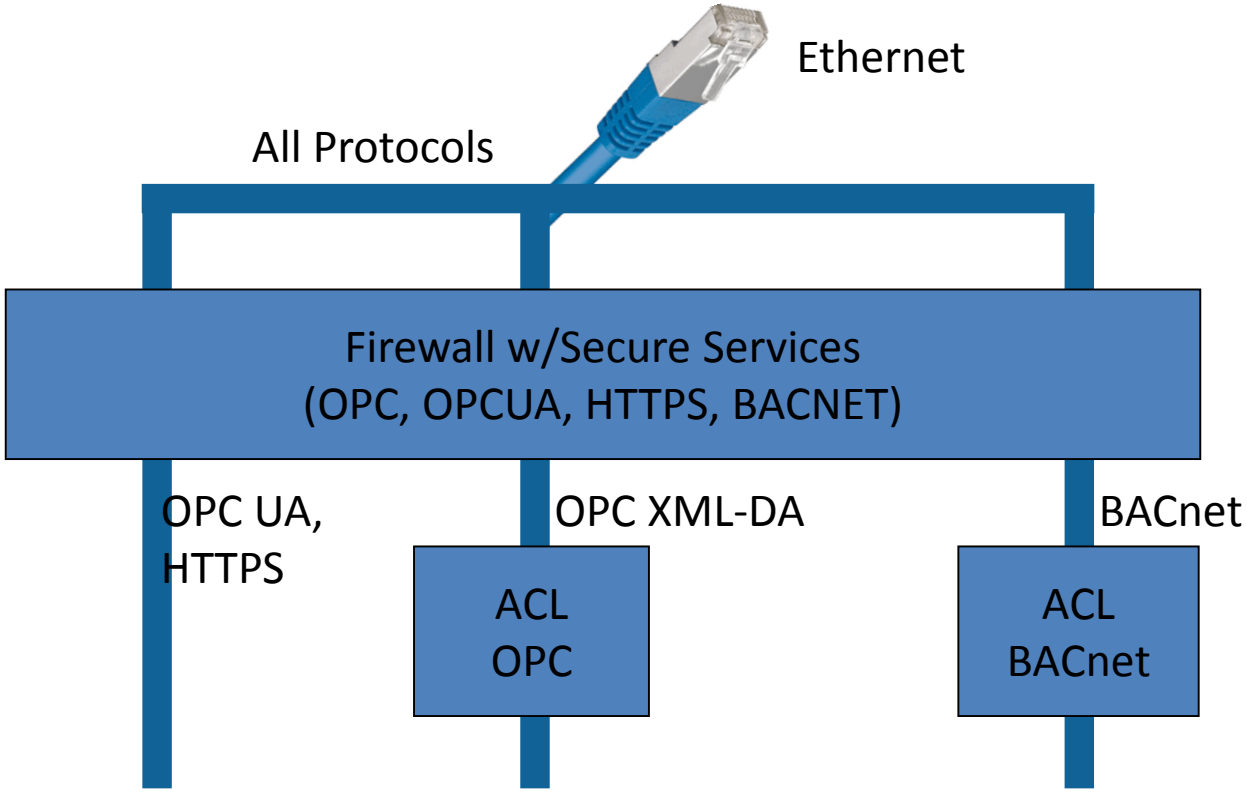
Change Passwords

Block Access

- Firewall (Secure Mode)
  - Block all insecure ports
  - Allow defined services
- Access Control Lists
  - Allow certain IP addresses
  - BACnet/IP (ACL)
  - LON (852 channel list)
  - Web Service (ACL)



Firewall and ACL



Secure Mode

- Configure Secure Mode
  - Turn on switch
  - Add secure services
  - Access over Web service

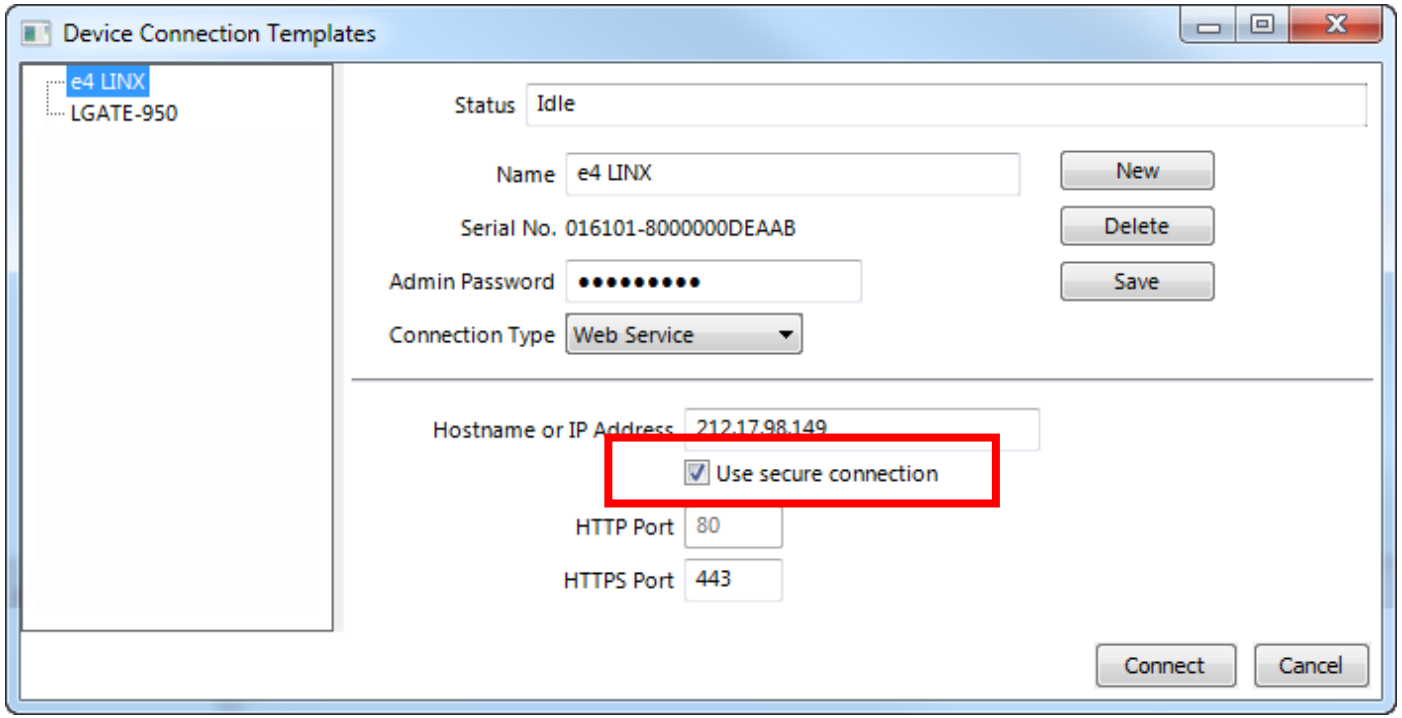
Secure Mode	input	binary	normal	active
Secure Mode_Set	output	binary	normal	active
Secure Services	input	string	normal	HTTPS OPC
Secure Services_Set	output	string	normal	HTTPS OPC

Secure Protocols

- Encryption
  - HTTPS: Web UI, Web services, configuration
  - OPC UA: BMS, Visualization
  - SSH: trouble-shooting
- Certificate Management
  - Pre-installed, self-signed
  - Server & CA (site)
  - Client certificates

Secure Configuration

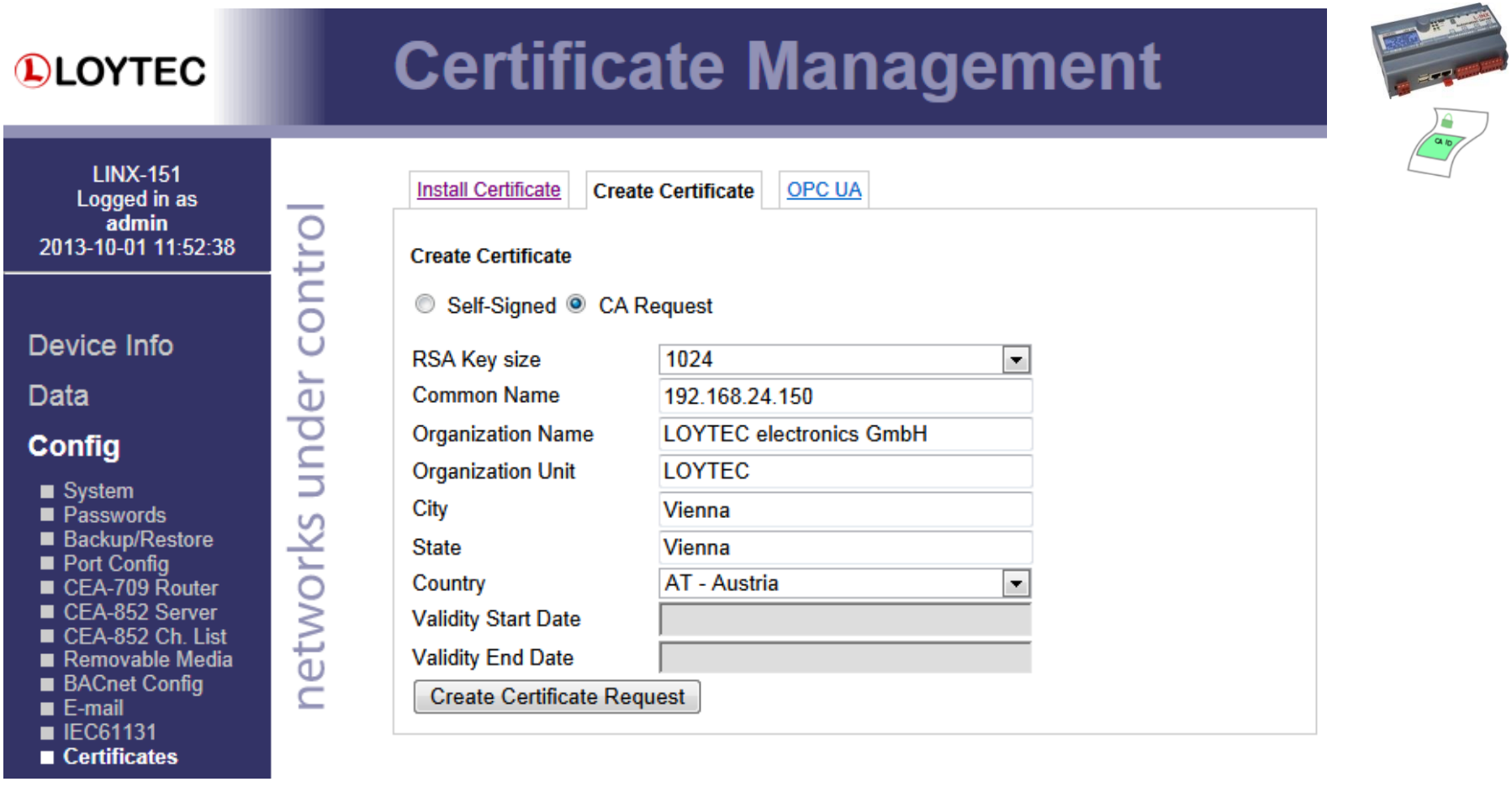
- Keep Passwords Secret
  - Use HTTPS on Web UI
  - Configurator secure connection



Server Certificates

- Create Site CA Certificate
- Sign Server Certificate
  - Use HTTPS
  - Create certificate request
  - Common name: IP address or DNS name
- Install
  - Server certificate on device
  - Site CA certificate on client

Sign Server Certificate (1)



Sign Server Certificate (2)

Install Certificate | **Create Certificate** | OPC UA

CA Request Pending

Certificate Request - Send to CA:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBsjCCARsCADBzMQ8wDQYDVQQHEwZWaWVubmExFzAVBgNVBAMTDjE5Mi4xNjgu
MjQuMTUwMQswCQYDVQQGEwJBVDENMAsGA1UEChMEQU1DTzEcMBoGA1UECxMTRmFj
aWxpdHkgTWFuYWdlbWVudDENMAsGA1UECBMETm9uZTCBnzANBgkqhkiG9w0BAQEF
AAOBjQAwgYkCgYEAyRJJL4aA7X4ircV6aL+WAAWxcdXm2PvIDKhjAIICHFh72X9k
08cbsxtk8ue18pqjar0TMKaGo/ezMX6O+Mt/4DPA142EhTMXpZGPdhS0HkdZaQi1
pkrblw9XV981G9ZJ+J8rValDTMtCGJCbUgMVmS/eBhqIlj30iLfJXVd0K00CAwEA
AaAAMA0GCSqGSIb3DQEBBQUAA4GBAA5vCxI0lY+dwwOHbHl4JZyorgkg0XkdRJnO
ZHTZrCtmIaHmV62eegnB8zoHGgGJR4OVFE4Rb+iJhowh11mGAt35aVebWHOsr7CX
ZhZqtCNNDJoPQ80FUHEQ/pRep3zEMEKIWHUBNw+F98TpR5kjWPhA4A3xC9v/9wtM
UkWxQe1v
-----END CERTIFICATE REQUEST-----
```

Certificate Request Reply - Paste reply from CA here:

Verify & Install | Cancel Request

Copy Request
Paste Response

Installed Certificate

Install Certificate | Create Certificate | OPC UA

Installed Server certificate	
RSA Key Size	1024
Validity Start Date	2013-10-01
Validity End Date	2016-07-21
Common Name	192.168.24.150
Organization Name	LOYTEC electronics GmbH
Organization Unit	LOYTEC
City	Vienna
State	Vienna
Country	AT
MD5 Fingerprint	C5:38:35:62:DE:F1:5D:84:7C:A5:C6:D8:18:7A:8E:BE
SHA1 Fingerprint	EB:10:4E:9C:46:78:17:90:1E:96:5A:2C:4A:04:60:E9:3E:6C:EF:C3

Install certificates (*.pem) :

Server certificate: Durchsuchen...

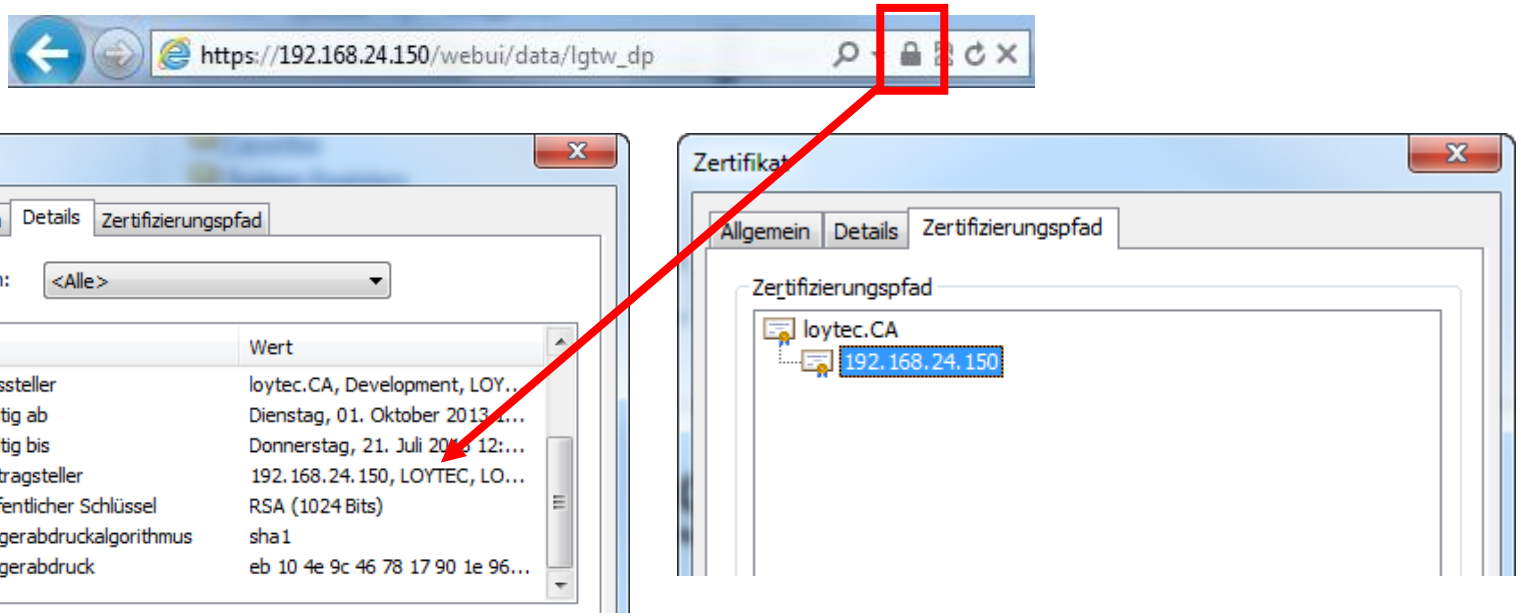
CA certificate: Durchsuchen...

Save | Reset certificates

Trusted Site Certificate

- Self-Signed Server Certificate

- Trusted CA Certificate



Securing CEA-852

- Integrity
  - Pre-shared key (MD5)
  - Channel delay against replay
  - Access control: channel list
- Confidentiality
  - Requires VPN solution

LonMark® International

Securing BACnet/IP

- Access Control
  - BACnet/IP ACL

BACnet Configuration

Device | Recipients | Time Master | BDT | **ACL** | Slave Proxy

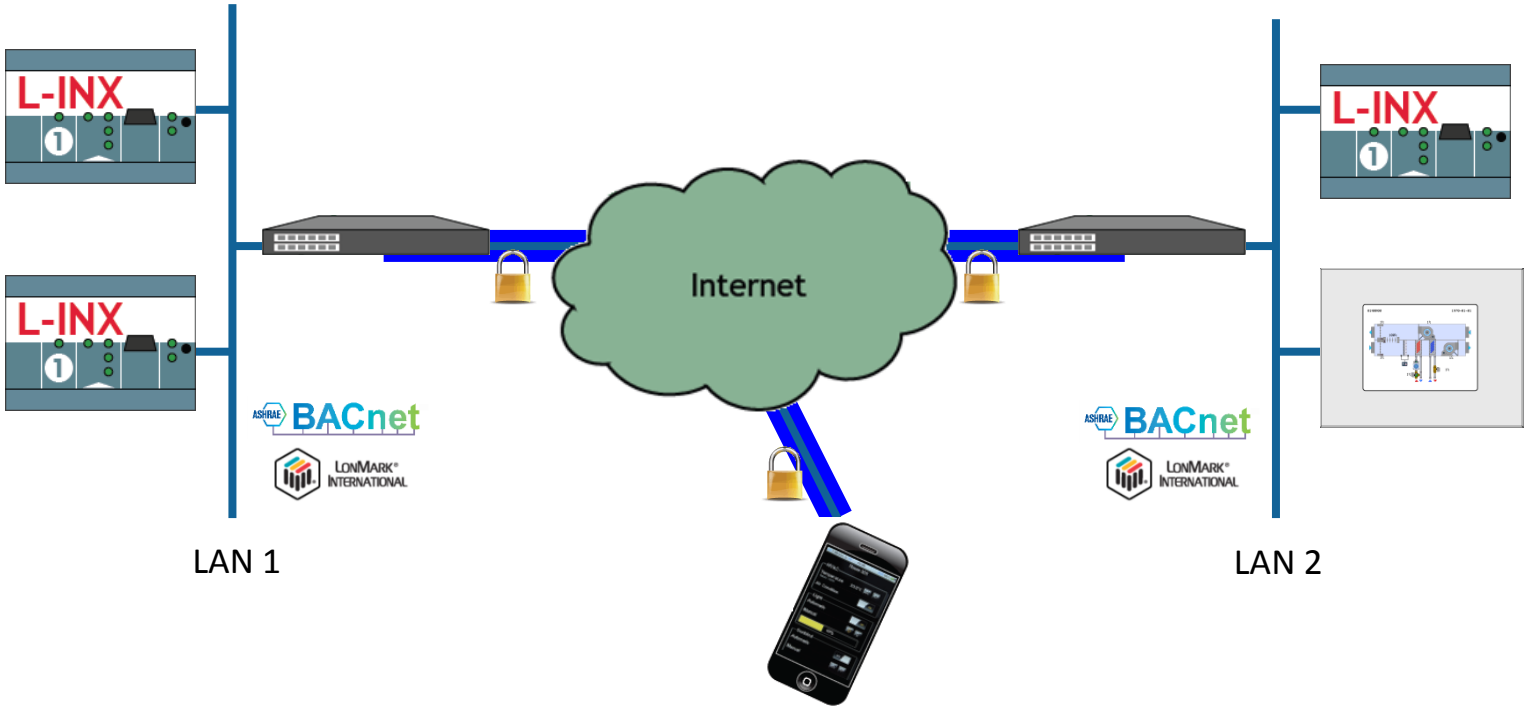
Add | Delete

IP Address	Subnet Mask	Access
10.101.17.2	255.255.255.255	allow
192.168.0.0	255.255.192.0	allow
0.0.0.0	0.0.0.0	deny

- Confidentiality/Internet
  - VPN solution

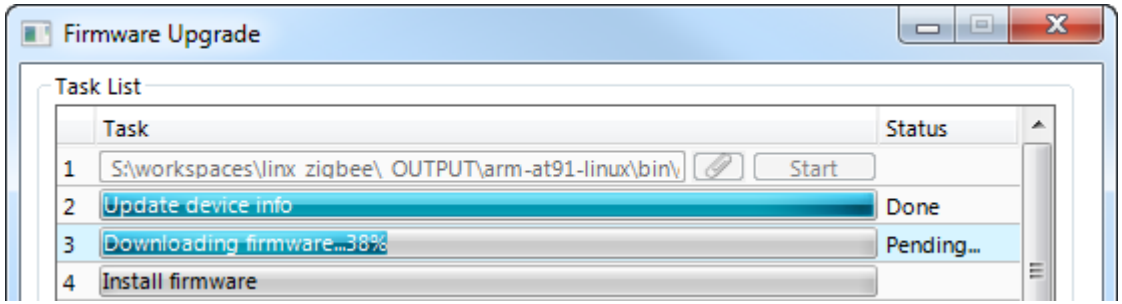
VPN Solution

- VPN Tunnel
  - Use VPN routers (IPsec, PPTP)



Security Updates

- Firmware Upgrades
  - Kernel updates for known security issues
  - Permanent checks with newest attack tools
  - Protects against exploits



Hardening Guide

- Hardening Guide
  - Turn off insecure protocols
  - Document open services
  - Logging (system log)
- Secure Mode
  - Hardening by one switch
- User Manual Appendix
  - Approved by GSA (U.S. General Services Administration)

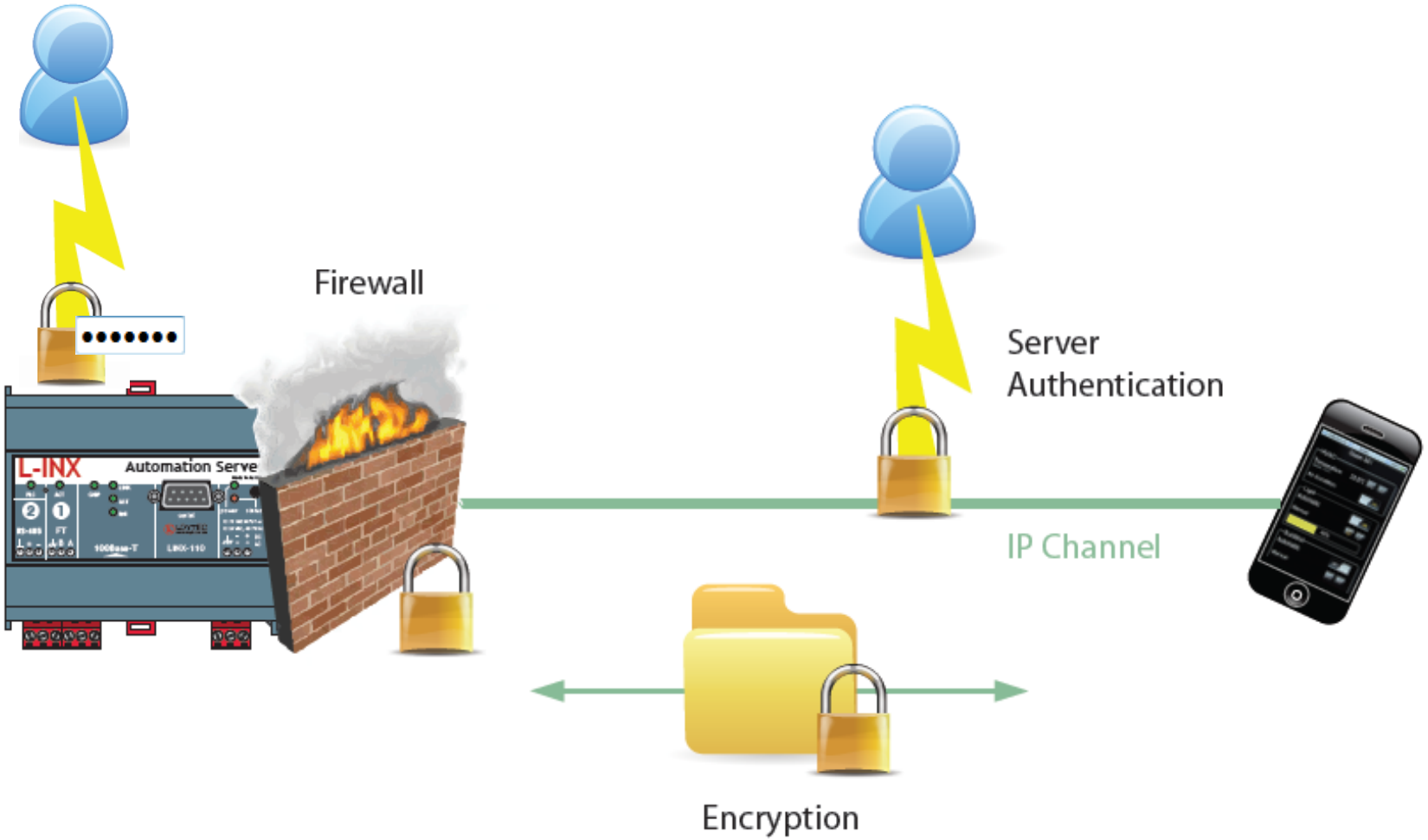
Select Models

- Security on some models:
  - L-INX: 12x; 15x; 22x
  - L-GATE: 95x
  - L-ROC: all models
  - L-VIS: 7”; 12”; 15”
- Refer to lock symbol in product catalog

Conclusion

- Security Built-In
  - Firewall
  - Secure protocols
  - Server authentication
- Hardening Made Easy
  - Flip the secure mode switch
  - Create server certificate
- Change Passwords!

Questions?


Firewall
L-INX
Automation Serve
Server
Authentication
IP Channel
Encryption